REMARKS/ARGUMENTS

The Examiner rejects claims 38-39, 47-54, 61-70, and 75 under 35 U.S.C.§103(a) as being unpatentable over Hankinson et al. (U.S. 6,799,202) in view of Williams (U.S. 6,304,973); claims 40, 41, 44-45, 55-56, 59-60, 71, and 73 under 35 U.S.C.§103(a) as being unpatentable over Hankinson-Williams in view of Kekic et al. (U.S. 6,763,370); and claims 42-43, 46, 57-58, 72, and 74 under 35 U.S.C.§103(a) as being unpatentable over Hankinson-Williams-Kekic and further in view of Schmeidler (U.S. 6,763,370).

Applicant respectfully traverses the Examiner's rejection. Independent claims 38, 53, and 69 are patentable over the cited references for at least the features highlighted below in the claims:

> 38. An arrangement for serving information requests, comprising:
> a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction and to provide a response to each transaction request; and
> a content director connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:
> a flow switch that parses plain text transaction requests to locate selected packet payload fields, selects, *based on the plain text packet payload fields,* an appropriate informational server to service each transaction request, and *thereafter* forwards at least portions of the parsed transaction requests to a selected one of the informational servers; and
> *a cryptographic module that decrypts, prior to parsing and informational server selection by the flow switch, cipher text transaction requests and provides plain text transaction requests to the flow switch, wherein, prior to decryption, the cipher text transaction requests have not been routed by another flow switch.*

53. In an arrangement comprising a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction, *to tag responses to transaction requests with a packet payload tag identifying uniquely the responding information server*, and to provide a response to each transaction request, a method for serving transaction requests from clients, comprising:

a cryptographic module decrypting a cipher text transaction request to provide a plain text transaction request to a first flow switch, the plain text transaction requests comprising a payload tag;

the first flow switch parsing the plain text transaction request to locate one or more selected fields *including the payload tag*;

the first flow switch, *based on the one or more selected fields,* selecting an appropriate informational server to service the transaction request; and

the first flow switch thereafter forwarding at least portions of the plain text transaction request to a selected one of the informational servers, *wherein the cipher text transaction request is decrypted prior to the parsing and selecting steps.*

69. An arrangement for serving information requests, comprising:

a plurality of informational servers connected to a communications network, all of the informational servers having a common address on the communications network and serving a set of information to clients, each of the informational servers being configured to receive a transaction request associated with an individual transaction, *to generate a corresponding tag identifying uniquely the generating informational server,* and to provide a response to each transaction request; and

a content director connecting the informational servers to the communications network and distributing transaction requests among the informational servers comprising:

first flow switching means for parsing plain text transaction requests to locate selected fields *including a generated tag*, selecting, *based at least in part on the generated tag*, an appropriate informational server to service each transaction request, and thereafter forwarding at least portions of the parsed transaction requests to a selected one of the informational servers;

decrypting means for decrypting, prior to parsing and informational server selection by the first flow switching means, cipher text transaction requests and providing plain text transaction requests to the first flow switching means, wherein, prior to the decrypting function, the cipher text transaction request has not been directed to a flow switching means other than the first flow switching means.

Conventional web switches have difficulty maintaining transaction coherency when a communication session with a client transitions from plain text (unsecured) to encrypted (secure) modes. To protect client/server communications from eavesdropping, tampering and message forgery, the Secure Sockets Layer (SSL) protocol is used to transport secured messages. The cookie in encrypted communications is also encrypted. When a transaction transitions from plain to cipher text, a new session ID is assigned to the transaction. Because the payload of the packet is encrypted, web switches assume that the next packet received from an IP address after the transaction becomes encrypted is a part of the immediately preceding clear text session with the same IP address. This assumption is not always correct. Many users, such as users behind a firewall or subscribers to an internet service such as Megaproxy™ offered by America On Line, can have the same global IP address. The encrypted sessions of such users can be crossed by the web switch, resulting in customer dissatisfaction and lost business. Web switches can also require excessive amounts of computational resources and otherwise suffer from computational inefficiencies.

The present invention can overcome this problem by positioning a cryptographic module between the communications network and the IP switch to selectively trans-crypt data within a secure HTTP transaction between a client and the network flow switch. The cryptographic module decrypts the packet before the packet is otherwise processed (*e.g.*, parsed) by the network flow switch and thereby identifies embedded destination and/or source invariants in the cipher

text portion of the packet. Frequently requested content can thereby be efficiently segregated and cached even among a cluster configuration of network flow switches.

Hankinson et al.

Hankinson et al. is directed to a high speed server in which different functions of the server's state machine are distributed across a plurality of processors running a plurality of operating systems. The web server has a number of members categorized into member classes. Each member class has a distinct specialized operating system that is optimized for its function. Load balancing (such as is performed by a traffic manager prior to routing by the flow switch) is performed without regard to the message contents prior to transmission of a message to a dispatcher 720 (col. 17, lines 41-50). With reference to Fig. 7 and col. 21, line 64-col. 22, line 8, an encrypted message is transferred from a receiver 745 (or input) to a dispatcher (or switch) 720. Dispatcher 720 then sends the message to another dispatcher 725 over a private connection 730. Dispatcher 725 then sends the message to a decoder 735, which decodes the message and returns the decoded message to dispatcher 725. Dispatcher 725 then sends a message identifying the location of the requested data to one of responders 740, and the responder 740 retrieves and sends the information to a decoder 735 for encryption and subsequently forwards an encrypted response, containing the encrypted information, to the client.

Hankinson et al. teaches the routing of the encrypted message first from a receiver 745 (which performs an initial analysis of the message) to a first dispatcher 720 and second from a first dispatcher 720 to a second dispatcher 725 *before the message is decrypted.* In contrast, the

claimed invention of claims 1 and 69 decrypts the message before it is initially routed by a switch, such as the receiver. The Examiner himself concedes that "Hankinson does not disclose encryption/decryption performed within the network interface and decryption completed prior to being routed by another flow switch." (Office Action at pages 3-4.) Accordingly, Hankinson et al. fails to address the problem noted above, namely how to distinguish transaction requests from different clients having a common address on the communications network.

Contrary to the Examiner's contentions, Hankinson et al. does not teach a tag generated by an informational server that identifies uniquely the generating informational server among the various servers in the server farm let alone positioning such a tag in the packet payload. At col. 11, lines 53-67, Hankinson et al. discloses using host names, IP addresses, and TCP port number to determine if the packet is part of a new or existing connection and the appropriate application to send the data to. This information is contained in the packet header, which is typically plain text.

The remaining references fail to overcome the deficiencies of Hankinson et al.

Williams

Williams, a newly cited reference, is directed to a security network 10 having a dedicated Network Security Controller (NSC) 12, workstations 14 and servers 16. The NSC 12 permits a security officer to configure and audit the operation of secure network 10. The network 10 also has security devices 18 installed between each host (workstation 14 or server 16) and the local area network medium 20. The various LANs 5 are connected to an untrusted backbone net 30 by

a router 22. The security device 18 operates at the network layer 3 of the protocol stack and provides encrypted, controlled communications from one host (IP address, TCP UDP port) to another. Each security device enforces a mandatory access control (MAC) policy and discretionary access control (DAC) on the packet flow to and from a host. It ensures labeling of all packets with a hierarchical security level and a set of non-hierarchical security categories. Finally, the security device 18 uses encryption to provide secrecy and communications integrity on all selected connections. Communications integrity mechanisms include keyed message digests, secure host algorithm, and message authentication code. All network communications pass through the security device 18 to access the network. In other words, the security device encrypts all messages automatically. The headers (IP, IPSec, CIPSO label, and cryptographic headers) are in clear text while IP data (i.e., TCP or UDP headers and data) are encrypted.

When a packet is received by the security device, it is placed in local RAM and MAC, DAC, decryption, and packet integrity functions are performed. For packets satisfying both discretionary and mandatory access control, the packet is decrypted using traffic key for source IP address, and the security device maps the packet out of the board memory and into the host (server) memory for provision to a workstation.

Williams fails to say how the mapping is performed; that is, Williams fails to disclose what fields are considered in mapping. Williams does not teach routing the decrypted packet to a switch for further routing to an information server. Moreover, Williams does not teach the use of a packet payload tag identifying a target information server for use in routing the packet.

Schmeidler et al.

Schmeidler et al. is directed to a system for secure delivery of on-demand content over broadband access networks that uses servers and security mechanisms to prevent client processes from accessing and executing content without authorization. A briq is mapped into a directory and file where it is stored in memory. In this manner, file system 1008 functions as an interface between the network request from the SCDP system and the memory 1050. Fig. 12 diagrams a briq. A briq 1200 includes a briq header 1202, a cryptoblock 1204, a superblock 1206, and one or more titles 1208A-N. A URN is a unique identifier of a title within a briq. The URN can correspond exactly to the current location of the title in the vendor's storage server. A URL identifies the current location of the briq in a RAFT storage server.

Kekic et al.

Kekic et al. is directed to a client-server management system using a combination of event rules and an event engine. In response to a selected event, a predetermined management action is undertaken.

Accordingly, the independent claims are allowable.

The dependent claims provide further reasons for allowance.

By way of example, dependent claims 39, 54, and 70 are directed to the simultaneous or near simultaneous receipt of encrypted transaction requests from different clients having a common electronic address on the network.

Dependent claims 40, 44, 45, 55, 59-60, 71, and 74 are directed to a hot invariant table identifying information frequently requested from informational servers. The Examiner points to Hankinson et al. to support the rejection of these claims. Hankinson et al. discloses the use of tables of IP addresses and host names to determine if the packet belongs to a new or existing connection and the appropriate application to send the packet to. Nowhere does Hankinson et al. state that the table tracks frequency of requests directed to selected information let alone a hit counter associated with the information. The same is true for Kekic et al. At col. 27, lines 12-18, Kekic et al. simply discloses the use of a threshold to determine if a rule is applicable and a specified action must be performed.

Dependent claims 42-43, 46, 57-58, 61, 72, and 75 are directed to the use of a digest value, for frequently requested information, to point to a location in the hot invariant table where objects regarding the information are stored. Although hashing is referenced at col. 18, lines 44-51, of Schmeidler, the hash code and an encryption key are used to digitally sign a launch string. The hash code is *not* related to a stored location of an object. It is a quantum leap to say that it is obvious, based on this teaching, to use a digest value to point to a location in the hot invariant where objects regarding the information are stored.

Dependent claims 49-52, 64-68, and 76 are directed to the switch tagging responses being forwarded to clients. Dependent claims 52 and 64 require the flow switch to operate in the taggging and digesting modes at different times. Hankinson et al. fails to teach or suggest both tagging and digesting let alone at different times.

Applicant wishes to clarify the intended meaning of certain claim language in light of the Federal Circuit decision "SuperGuide Corporation v. DirecTV Enterprises, Inc., et al., 358 F.3d 870 (Fed. Cir. 2004). In that decision, the Federal Circuit held, under the unique facts of that case, that the phrase "at least one of a desired program start time, a desired program end time, a desired program service, and a desired program type" means "at least one of a desired program start time, at least one of a desired program end time, at least one of a desired program service, and at least one of a desired program type".

Applicant has used the phrases "at least one of . . . and" and "and/or" in a number of claims and wishes to clarify to the Examiner the proper construction of this phrase. Applicant intended the phrases "at least one . . and" and "and/or" as used in the claims to be an open-ended expression that is both conjunctive and disjunctive in operation. For example, the expressions "at least one of A, B and C" and "A, B, and/or C" mean A alone, B alone, C alone, A and B together, A and C together, B and C together, and A, B and C together. Applicant believes that this construction is consistent with the Examiner's construction of the claims in the Office Action. If the Examiner disagrees with this construction, Applicant respectfully requests that the Examiner notify Applicant accordingly so that Applicant can further amend the claims.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

SHERIDAN ROSS P.C.

By:_____

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: _____

J:\4366\-49\Amendment and Response-002 (9-05).wpd